МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 27-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ
«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

10 – 12 травня 2023 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2023

УДК 004:[621.317+621.391](06)

27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – 192 с.

В збірник включені матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

УДК 004.77:004.056

РОЗРОБКА ПРОГРАМНОГО МОДУЛЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ МЕСЕНДЖЕРА

Майба М.А.
Науковий керівник – д.т.н., проф. Єременко О.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(099) 640-59-37, e-mail: mykola.maiba@nure.ua.

This work is dedicated to developing a software module that enhances the security of personal data when using Telegram messenger. Various approaches can be used to create such a software module. This paper examines a hybrid method of information protection that involves the use of data encryption and steganography. By using the software module, protection against intruders who may attempt to intercept transmitted messages is provided. If an intruder intercepts the data or the messenger team cooperates with other entities and transfers data to third parties, the user's security will not be affected since the content of the correspondence will be impossible to read.

Для підвищення безпеки персональних даних користувача було реалізовано програмний модуль для безпечної передачі інформації з використанням відомого месенджеру Telegram, який заздалегідь шифруватиме повідомлення за допомогою стеганографічного алгоритму Steg Cloak [1, 2]. Побудована програма складається з чотирьох основних модулів: MAIN, START, TRANSF та STEG. Модуль MAIN являє собою основу структури програми, яка викликає інші модулі у правильній послідовності. Перший модуль який буде викликаний модулем MAIN – це START. Він створює таблицю MySql, в якій буде зберігатися API нашого клієнта, дані співрозмовника та наші власні дані.

Далі у модулі необхідно ввести реєстраційні дані для генерації клієнта Telegram, а саме API ID та API HASH. Ці дані можна отримати на офіційному вебсайті месенджера. Після цього нам необхідно ввести логін співрозмовника, з яким користувач буде вести діалог. Всі ці дані додаються до бази Info.db. Модуль TRANSF потрібен для обміну повідомленнями між двома користувачами. Після заповнення бази буде створено дві Telegram сесії клієнта. В межах однієї сесії ми зашифровуємо повідомлення та надсилаємо отримувачу, а в межах іншої – розшифровуємо його повідомлення.

Для зашифрування та розшифрування використовується четвертий модуль STEG. Для цього використовується алгоритм стеганографічного шифрування StegCloak, здатний зашифрувати повідомлення за алгоритмом AES256. Потім він стискає отриманий результат і перетворює його на

спеціальні Unicode символи, ці символи вставляються всередину повідомлення та не привертають уваги.

У модулі STEG реалізовано взаємодію з сервісом StegCloak у вигляді командного рядка, а сама зашифровка або розшифровка повідомлення здійснюється за допомогою керування конфігураційними JSON файлами. Алгоритм роботи сервісу StegCloak проаналізовано у [1, 2].

Також під час виконання програми використовуються сторонні бібліотеки, які розширюють стандартний функціонал та дозволяють обробляти великий об'єм даних, серед яких [3, 4]:

1. Бібліотека telethon, яка призначена для спрощення написання програм мовою Python, які можуть взаємодіяти з Telegram. Використовується для відправки повідомлень.
2. Бібліотека Tkinter як стандартний набір інструментів з графічним інтерфейсом для Python. Використовується для графічного виведення повідомлень, які користувач надсилає або отримує.
3. Бібліотека pysqlite3 – бібліотека, яка надає полегшену базу даних на диску, не потребує окремого серверного процесу і дозволяє звертатися до бази даних з використанням нестандартного варіанта мови запитів SQL.
4. Бібліотека lorem-text – бібліотека для генерування супровідного текста.
5. Бібліотека asyncio, що використовується як основа для декількох асинхронних фреймворків Python, які забезпечують високопродуктивні мережні та веб-сервери, бібліотеки підключення до баз даних, розподілені черги завдань тощо.

Тестування розробленого модуля підтвердило його працездатність та ефективність.

Список використаних джерел:

1. Білокуров, О. О., Майба, М. А., Шлома, О. К., & Дробяз, М. О. (2022). Аналіз методів захисту інформації, що знаходять використання у сучасних месенджерах. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2022)». Харків, ХНУРЕ, 2022. 71–73. https://openarchive.nure.ua/handle/document/21190

2. GitHub – KuroLabs/stegcloak: Hide secrets with invisible characters in plain text securely using passwords. (n.d.). GitHub. https://github.com/KuroLabs/stegcloak

3. Telethon's Documentation – Telethon 1.27.0 documentation. (n.d.). Telethon's Documentation – Telethon 1.27.0 documentation. https://docs.telethon.dev/en/stable/

4. asyncio Asynchronous I/O. (n.d.). Python documentation. https://docs.python.org/3/library/asyncio.html